AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

USAF EXPEDITIONARY SECURITY OPERATIONS 2040: A TECHNOLOGY VISION FOR DEPLOYED AIR BASE DEFENSE CAPABILITIES

by

Christopher W. Allen, Major, USAF

Blue Horizons

Advisors: James K. Selkirk, Jr., Commander, USN
Thomas E. Kiesling, Major, USAF

9 April 2014

DISCLAIMER

ABSTRACT

This research paper envisions specific United States Air Force (USAF) "Expeditionary Security Operations" (ESO) capabilities and enabling technologies in the 2040 timeframe. Technological advances provide opportunities to increase future USAF capabilities to conduct base security and counter-threat operations (CTO) to protect forward bases from ever-evolving challenges and threats to deployed personnel and assets. Although individual ESO capabilities and technologies may seem relatively insignificant standing alone, the ability to secure personnel, aircraft, and equipment is all-important to USAF force projection in the future.

Using analysis of state-of-the-art ESO technologies, this research paper advocates for leveraging improvements in technology trends in order to satisfy specific ESO capabilities requirements in 2040. For base security, laser-based counter-indirect fire (IDF) systems will autonomously defeat precision IDF projectiles with increased accuracy and range, while minimizing collateral damage risks. A variety of autonomous and remotely-operated unmanned ground vehicles (UGVs) carrying sensors and weaponry will enhance inside-the-wire protection and response capabilities. Non-lethal robotic sentries equipped with sensors and weaponry will autonomously detect and defeat violent insider threats.

For CTO, UGVs of sufficient survivability and load capacity will augment manned convoys and thereby enhance outside-the-wire travel and sustainment by carrying sensors and weaponry necessary for convoy security. Directed energy weapons will improve vehicle convoy and foot patrol protection by adding effective use of force options. Speech-to-speech language translation devices will enable more communications by CTO personnel with more local individuals to rapidly obtain perishable, vital threat information.

TABLE OF CONTENTS

Introduction

In the not-so-distant future, the President orders the United States military to conduct combat operations against a hostile state to protect national interests. American forces succeed in overcoming advanced anti-access/area denial measures and establish new expeditionary air bases from which the US Air Force contributes manned and unmanned sorties to the joint fight. However, the enemy employs novel asymmetric tactics to hinder, harass, and deny USAF power projection. Precision indirect fire, remotely-piloted vehicles, sophisticated insider attacks, and other innovative enemy capabilities ceaselessly wreak havoc on the bases, threatening to halt critical USAF missions . . .

Mindful of this future worst-case scenario, the USAF will undoubtedly be called upon to deploy forces to conduct operations around the world in the next three decades—based on the frequency of expeditionary missions in the past three decades. The importance of base defense in hostile areas endures and requires improvement to meet ever-evolving threats in the future. This research paper envisions specific USAF "Expeditionary Security Operations"[1] (ESO) capabilities and enabling technologies in the 2040 timeframe. Technological advances provide opportunities to increase future USAF ESO capabilities in order to protect forward bases from ever-evolving challenges and threats to deployed personnel and assets. Current decisions and planning must be influenced toward research, development, and acquisition in specific technology areas to enhance future ESO.

To explore ESO, the first section explains the research methodology so it is clear how future capabilities and technologies will be examined. The second section discusses the doctrinal context of how the USAF secures its bases, specifically the roles of base security and counter-threat operations (CTO) in ESO. The relevance of future ESO capabilities and technologies to

national defense interests is also briefly articulated to emphasize the importance of proper planning and procurement to protect future USAF bases from future threats. The third section identifies projected capabilities for future base security and CTO requirements. The fourth section discusses technological advances to meet anticipated base security and CTO capabilities requirements. The final section offers overall recommendations for ESO procurements to posture future base security and CTO capabilities to overcome challenges and defeat anticipated threats in 2040.

Research Methodology

This research effort offers capabilities for effective ESO in the next thirty years based on expected challenges and threats. Capabilities identification allows for exploration of technologies to meet future ESO needs, bearing in mind the simultaneous need to anticipate threats that may counter or negate future ESO technologies and capabilities. Specifically, each technology section first links to a specific capability projected to counter or defeat a threat(s). Next, various existing technologies or systems are introduced and assessed with respect to strengths and weaknesses. Lastly, recommendations for technology enhancement are presented within each section. Overall, the intent of this research effort is to identify and analyze state-of-the-art ESO technologies, and ultimately advocate for leveraging improvements in technology trends in order to satisfy specific ESO capabilities requirements in 2040.[2]

ESO Doctrinal Background and Relevance

Doctrinally, the USAF uses the terms "force protection," "integrated defense," and "force protection intelligence" to explain missions and capabilities needed to secure Airmen and resources from threats and harm, stateside and abroad. Force protection is "[t]he process of detecting threats and hazards to the Air Force and its mission, and applying measures to deter,

pre-empt, negate or mitigate them based on an acceptable level of risk."[3] Integrated defense is a force protection line of effort. USAF Security Forces are the "enterprise lead" for integrated defense, which operates to "protect and defend Air Force personnel, installations, activities, infrastructure, resources, and information . . . worldwide, from mature theaters to austere regions."[4] Force protection intelligence (FPI) is vital to integrated defense. FPI leverages the efforts of USAF intelligence, Security Forces, and AFOSI personnel to collectively provide a threat sight picture that enables leaders at all levels to enact proper force protection measures.[5]

It is important to understand how integrated defense and FPI are operationalized in a deployed environment to execute what can be termed ESO.[6] Security Forces, or "Defenders," use the full spectrum of defensive ways and means to provide base security "to mitigate potential risks and defeat adversary threats to Air Force operations within the Base Boundary (BB) and the Base Security Zone (BSZ) in order to ensure unhindered AF operations."[7] Defenders conduct patrols to deter and detect threats to personnel and resources, and man static posts at entry control points (ECPs) to regulate entry and exit from an installation. Defenders respond to defeat threats when they emerge within the BB ("tactical or jurisdictional limit"), and can also do so in the BSZ ("range of enemy capabilities") depending on the host nation relationship.[8] This includes indirect fire (IDF) threats from rockets, mortars, and man-portable air defense systems (MANPADS). Defenders leverage technologies to track and interdict IDF threats before they strike, and aerial assets assist with efforts to locate and defeat attackers.

AFOSI CTO activities play a vital role in supporting integrated defense and FPI to protect expeditionary bases through use of "capabilities to find, fix, track, and neutralize enemy threats in order to create a sustained permissive environment"[9] for deployed airpower. Collection, analysis, and dissemination of timely, multiple source information provides pertinent

authorities "tactical situational awareness to forewarn or preempt enemy or adversarial attack[s]"[10] against aircraft, personnel, and infrastructure.

Counterintelligence collections are the core CTO activity. Primarily, this means recruiting, handling, and extracting threat information from human sources. In an expeditionary environment, human sources of information can be found among the base populace—including local or foreign nationals granted access—but it is also important to locate and meet sources who reside or work within the BSZ. To do so, AFOSI personnel must travel off the installation to local population centers to canvas areas for new sources or to meet existing sources. In uncertain or hostile BSZ environments, AFOSI units partner with Security Forces "Tactical Security Element" (TSE) teams to conduct and secure CTO missions. TSE members transport agents, linguists, and support personnel in tactical vehicles with significant defensive firepower and the capacity to carry equipment and supplies necessary for convoy security and sustainment.

While tactical in execution, ESO is relevant to strategic interests. Events over the past thirty years indicate the military instrument of power is likely to see continued use in a variety of operations at different levels of conflict over the next thirty years. USAF power projection requires basing in areas of operation. Expeditionary bases enable USAF combat operations to support national security priorities; at the same time, bases represent highly visible targets for enemy attacks. Preventing or minimizing attacks on bases is important for mission continuity, but also to prevent enemy propaganda victories from successful attacks and to avoid negative impacts on American public support for war efforts.[11] These challenges are unlikely to diminish, and necessitate adequate development of capabilities and technologies to confront future threats from increasingly sophisticated competitors.

Future Capabilities Requirements

Capabilities rely on means to provide the ability to conduct activities that create effects toward objectives. For ESO, three specific base security capabilities will be important in the future based on a dynamic, ever-challenging threat environment:

1. *The ability to more effectively counter indirect fire threats to expeditionary bases.* Rocket, mortar, and MANPADS capabilities will only increase in targeting precision, accuracy, and lethality in coming years.[12]
2. *The ability to more effectively monitor, patrol and respond within the BB to improve perimeter and ECP protection.* This counters enemy tactics which continually increase in effectiveness against human and technical security measures, while also responding to future remotely-piloted ground vehicle threats.[13]
3. *The ability to more effectively detect, interdict, and neutralize violent insider threats.* The continued use of local nationals for support at deployed bases is anticipated, with attendant risks of enemy infiltration among such employees. Additionally, threats from “friendly” individuals unfortunately continue to emerge in deployed locations.[14]

Three specific CTO capabilities will counter future threats to expeditionary bases[15]:

1. *The ability to more effectively travel outside-the-wire within the BSZ to meet individuals to obtain counter-threat and atmospherics information on areas in close proximity to a deployed base.* Rugged, austere environments and creative enemies will continually challenge CTO convoy mobility.
2. *The ability to more effectively use non-lethal and lethal means to protect CTO vehicle convoys and foot patrols.* Rules of engagement that allow for local vehicles to travel in close proximity to convoys are assumed. Creative enemies will be relentless in

efforts to attack convoys. Crowd control will pose an ever-evolving threat to foot patrols, especially in densely populated, confined spaces.

3. *The ability to effectively communicate with more local individuals to obtain increased threat and atmospherics information for areas in close proximity to a deployed base.* Currently, one or two linguists facilitate communication with a limited number of locals during an engagement visit. Language training for CTO personnel is very limited and rarely sufficient to allow adequate understanding of complex descriptions of threats, individuals, etc.

The aforementioned base security and CTO capabilities[16] depend on improvements in existing technologies or new technologies to bring future ESO capabilities to fruition. Technology is operationalized scientific knowledge; it provides a capability in the form of a tool. Technological advances drive development of various systems, enabling improvements in base security and CTO capabilities to meet future threats.

Future Base Security Technologies

Future base security capabilities require technological innovations in counter-IDF systems, unmanned ground vehicles (UGVs), and robotic sentries. Counter-IDF systems will leverage various technologies to increase accuracy and range in destroying inbound projectiles targeting an expeditionary base. UGVs of various sizes will enhance perimeter security and entry control point protection, and conduct inside-the-wire security patrols. Robotic sentries will protect key base facilities and highly-populated areas from violent insider threats. While UGVs and robotic sentries are not the only means to improve specific future capabilities, advances in these technologies offer opportunities to "enable manpower efficiencies and cost reductions."[17]

Counter-IDF Systems

Ground-launched projectiles pose a significant threat for base security. Frequent insurgent IDF attacks on Coalition bases in Iraq prompted adaptation of the US Navy Phalanx—a Gatling gun-based anti-ship missile system—into the Centurion Counter-Rocket, Artillery, Mortar (C-RAM) system to autonomously defend a 1.2 km square area around deployed bases.[18] IDF attacks have also been a constant source of concern for NATO bases in Afghanistan. C-RAM systems shot down approximately 70 percent of IDF in both conflicts.[19] Overall, imprecise IDF caused more fear and harassment than actual death and destruction, a fortunate outcome that is not likely to continue.[20] In the future, "[s]hould precision IDF rounds become part of the operational environment, our Airmen won't have the luxury of an enemy's incompetent firing of dumb rounds"[21]—an apt caution indeed. Moreover, a 30 percent failure rate will not suffice against future precision IDF attacks. Future threats of increasingly precise IDF demand a more effective counter to protect deployed resources.

Other recent counter-IDF technologies include the German Skyshield air defense system. Similar to the Centurion, Skyshield uses revolving guns to provide a C-RAM capability. Unlike the Centurion, Skyshield munitions do not directly strike the targeted projectile. Skyshield rounds containing numerous subprojectiles are fired into the calculated path of the target, creating a destructive field of fire.[22] This method offers the ability to strike targets at greater distances with less ammunition expended.[23]

Additional counter-IDF technological developments include Israel's Iron Dome C-RAM system. The Iron Dome uses interceptor missiles to protect population centers against multiple, simultaneous IDF threats within a 70 km zone.[24] According to US and Israeli officials (both countries financed its development), Iron Dome's accuracy rate in destroying inbound projectiles

is between 80 and 85 percent as of 2012.[25] Meanwhile, Raytheon recently explored a laser-based version of the Phalanx and Centurion to enable defense of a larger area, about three times the area protected by existing systems, at lesser expense compared to a Gatling gun or missile-based C-RAM.[26] Requirements for a laser version of the Centurion include sufficient power to defeat larger IDF threats, ruggedness to effectively operate in harsh environments, and friendly aircraft avoidance.[27] These concerns stem from the developmental experiences of other laser-based C-RAM systems.

In 1996, the US and Israel began joint development of a Tactical High Energy Laser (THEL) to protect Israel from IDF. After ten years of work and $300 million spent, the chemical-based laser program was terminated due to the system's "bulkiness, high costs and poor anticipated results on the battlefield."[28] More recent counter-IDF development has focused on electric lasers, which hold the promise of increased targeting precision and speed. Specifically, Boeing is developing the High Energy Laser Technology Demonstrator (HEL TD) for the U.S. Army, an eight-wheeled tactical vehicle with a solid-state laser designed to defeat IDF, remotely piloted aircraft (RPA), and other tactical airborne threats.[29] A potential limiting factor is the ability to continuously generate sufficient electricity to power the laser in an austere environment.

Future counter-IDF systems, whether based on missile, laser or other directed energy technologies, must increase in accuracy and range in order to autonomously destroy multiple inbound projectiles targeting an expeditionary base. These systems must also minimize collateral damage risks to friendly aircraft and populations. As laser technologies continue to mature into more powerful, smaller systems requiring less energy, effective laser-based counter-IDF systems with "near-infinite magazines" will be an attractive option in 2040 in terms of cost

and risk mitigation to surrounding ground communities.[30]

Unmanned Ground Vehicles

UGVs have yet to be fully exploited for base security.[31] Existing and developing UGV technologies hold significant potential to provide effective capabilities for perimeter, ECP, and inside-the-wire protection. A sensor-carrying UGV provides "eyes and ears" without the need for a human on site. Multiple UGVs create a network for base defense operations center personnel to monitor in order to respond to threats.

Recent UGV technological developments include the Mobile Detection Assessment Response System (MDARS), which affords the US Army and Navy a capability "to provide fixed site security by autonomously patrolling an area and detecting intruders."[32] Larger than a "four-wheeler" all-terrain vehicle, MDARS avoids obstacles and can operate non-stop for sixteen hours to conduct "autonomous, random patrol missions as scheduled, or [it] can be remotely operated by joystick."[33] Its control station enables operation of up to sixteen vehicles at once, creating a "small and nimble robotic patrol force on wheels."[34] In 2004-05, Hawthorne Army Depot, NV, the largest US Army munitions storage facility, successfully tested MDARS. Four vehicles logged 2000 patrol hours and traveled 10,000 miles.[35] A follow-on program, MDARS II, seeks to use software and hardware to convert commercial and military vehicles into unmanned sensor platforms.[36] MDARS II also envisions the ability to carry and control "less lethal response capabilities."[37]

The Israeli Guardium is a currently-fielded UGV. Modified from a commercial off-road vehicle, it is slightly smaller than a WWII-era Jeep. Guardium is a mobile reconnaissance sensor platform (with a loudspeaker), often used in conjunction with foot patrols to detect and deter threats along the Gaza Strip security fence.[38] It is also used for tactical resupply to eliminate

improvised explosive device (IED) threats to manned vehicles, and retains the "possibility to install a Remotely Operated Weapons System and Non-lethal Weapons Systems."[39] Interestingly, the next Guardium will be "a bigger Ford F-350-based model with a weapon mounted on top."[40] Unlike the small MDARS or MDARS II conversion kits, Guardium foreshadows a full-size UGV that can discreetly integrate with and augment manned vehicle and foot patrols, or operate on its own to conduct deterrence, detection, and response missions without risking the lives of friendly forces.

Current and developing systems offer a glimpse of UGV possibilities in 2040. UGVs can be the same size, model, color, etc., as manned vehicles when used for patrols or as reinforcements at static locations. This will confuse insider threats regarding which vehicles are manned, providing an additional defensive variable for enemies to overcome. Additionally, small UGVs will navigate hard-to-reach places and decrease presence visibility. While mounted cameras at key locations provide great visibility and "zoom" with ever-increasing effectiveness, static cameras are unable to see around obstructions, making a small, mobile UGV valuable. RPAs are also obviously useful for this, but the ground view from a UGV provides a more relatable perspective for response purposes, including reaction to enemy penetration of a base. Lastly, MDARS provides a preview of "swarming" multiple small UGVs to quickly respond in suitable numbers to a threat to provide situational awareness, employing non-lethal and/or lethal force as appropriate. Such threats could include "[p]rotestors, mobs, and terrorist groups . . . quickly assembling near a base's entry-control point or perimeter to protest, riot, or attack."[41]

<u>Robotic Sentries</u>

Robotic sentries or "sentry-bots"[42] can also thwart attacks at the base perimeter. In fact, UGV technological developments are closely related to robotic sentry advances, since UGVs

armed with lethal and/or non-lethal weapons can assume a static posture at specific locations to detect and neutralize violent insider threats. Robotic sentries can conceivably use sensors and facial recognition technologies to check identification to permit or deny entry to various locations.[43] The most interesting recent robotic sentry technological developments come from South Korea and Israel.

Samsung Techwin built the SGR-A1 sentry for use on the South Korean side of the demilitarized zone (DMZ).[44] As a stationary surveillance and response platform, the SGR-A1 avoids "the power, communications, and traction issues which tend to plague its mobile [UGV] counterparts."[45] Multiple sensors alert human operators to respond in person, or the SGR-A1's operator can warn potential attackers via loudspeaker, track multiple targets, and engage using lethal (5.56 mm machine gun) or non-lethal weaponry (rubber bullets).[46] The Super aEgis 2 is another South Korean DMZ sentry. Like the SGR-A1, the Super aEgis 2 can detect, track, and engage targets up to three kilometers away.[47] Its all-weather automatic turret supports lethal weapons—machine guns, grenade launchers, or surface-to-air missiles.[48] For the Gaza Strip border, the Israelis erected Sentry Tech towers equipped with sensors and lethal weapons "to create 1500-meter deep 'automated kill zones.'"[49] A single operator controls multiple towers, reducing manpower requirements and decreasing risks to human responders.[50]

For the USAF, the idea of a non-lethal robotic sentry appears less risky and offers a higher likelihood of use in 2040. Autonomous sentries posted among "friendlies" at densely-populated locations (ECPs, dining facilities, gyms), critical mission areas (command buildings, flightlines), and critical infrastructure sites (communications nodes, power generation facilities) provide a key element of an effective future "comprehensive interior security plan"[51] to defeat violent insider threats. Additionally, incapacitating—not killing—an insider threat enables

subsequent intelligence or law enforcement information collection from an individual(s).

Future CTO Technologies

Future CTO capabilities require technological advances or innovations in unmanned convoy vehicles, directed energy weapons, and language translation devices. UGVs will augment manned convoy vehicles to provide security support, carry supplies and equipment, and deliver humanitarian aid to local populations in efforts to win their support. Directed energy weapons—non-lethal and lethal—will provide more use of force options for CTO convoys and foot patrols. CTO personnel on the ground will use language translation devices to communicate with more local individuals, in order to more effectively gain potential threat information to prevent attacks.

Unmanned Convoy Vehicles

UGVs will augment manned CTO convoy vehicles to enable safer, more effective outside-the-wire travel to meet individuals—and deliver humanitarian aid when appropriate—in order to obtain threat information. UGVs enhance the protection and sustainment of CTO convoys by carrying additional sensors and weaponry, as well as equipment and supplies, without necessarily expanding manpower requirements. Two recent systems—the Guardium and the Crusher—provide a preview of future UGV convoy support.

As previously discussed, the Israeli Guardium is an off-road, all-terrain vehicle capable of incorporation into convoys that travel unimproved surfaces and traverse rugged terrain. It operates semi-autonomously at speeds up to 50 kilometers per hour and carries up to 1.2 tons in supplies and equipment.[52] Operators control Guardium via a stationary, mobile, or portable control terminal,[53] which suggests it can be controlled from a deployed base or from inside another manned vehicle within a convoy. If operated from base, a variable of concern is the

maximum distance of control from a stationary control terminal based on the robustness of its wireless communication in a variety of climates and terrains. Additionally, its unmanned nature significantly mitigates survivability concerns, but it is unclear what level of fire Guardium can endure and still function. This is important if the UGV is relied upon for fire support to the convoy, as well as for transport of vital supplies and equipment. These concerns may be answered in the near-term in a couple of ways: the next Guardium will be the size of a Ford F-350[54] and the Guardium "Autonomous Kit could easily be migrated to different types of vehicles, based on customer's preferences."[55] Theoretically, Guardium technology holds the possibility of use on existing and future USAF tactical convoy vehicles.

In 2006, Carnegie Mellon University's National Robotics Engineering Center (NREC) introduced the Crusher, a seven-ton, six-wheel hybrid engine UGV. The Crusher provides a ruggedized, highly-versatile off-road chassis to prove autonomous UGV capabilities to perform various tactical tasks, including reconnaissance and surveillance, re-supply, and convoy defense, in a combat environment. It can carry over 8,000 pounds of payload and armor, a significant capacity to transport equipment, supplies, sensors, weaponry, etc. The Crusher operates via multiple control modes—including full autonomy—and travels at speeds up to 26 miles per hour. Interestingly, its hybrid diesel/electric engine enables relatively quiet movement for a large tactical vehicle in rough terrain.[56] While slower than the much smaller Guardium, the Crusher appears to be significantly more survivable and carries over six times the payload. Still, the Crusher's developers acknowledge the need to remedy specific areas of concern, including safety (especially due to its size), communications and navigation, and overall operation and supervision of the UGV and its payload.[57]

The Guardium and Crusher show great potential for future UGV integration into tactical convoys, though advantages and disadvantages are evident in both systems. The NREC believes UGV research and development will ultimately, "enable new war-fighting capabilities while putting fewer soldiers in harm's way."[58] The intent with respect to future UGV incorporation into CTO convoys is no different: more capabilities with less risk to Airmen on the ground. While a UGV must be able to traverse the same rugged, austere terrain as manned tactical vehicles, its principal advantage within a convoy is the elimination of the need for an on-board human driver and multiple other occupants, removing targets for enemies to threaten. The UGV operator rides in another manned vehicle in the convoy or controls the UGV from base. Ideally, a UGV will also operate autonomously within a convoy in 2040 as a "doppelganger," mimicking manned convoy vehicle movements based on programming for speed, distance, etc.

<u>Directed Energy Weapons</u>

Powerful lasers hold great promise for defeating IDF threats to deployed bases.[59] On a different level, lasers and other directed energy weapons offer future possibilities for non-lethal and lethal applications against individual and vehicle threats posed to CTO convoys and foot patrols. Currently, directed energy weapons enable the ability to disable a threatening vehicle approaching a convoy, or dissuade a threatening individual(s) in the vicinity of a foot patrol. Future advances in directed energy weapons will enhance these capabilities, potentially providing lethal options as well.

Recent directed energy weapons include various "optical distractors" or "dazzlers," which "deliver flash and optical glare effects to deny access, move, or suppress individuals."[60] Models currently in use include the hand-held or weapon mountable LA-9/P and GLARE MOUT, with ranges of 65-1000 meters and 18-760 meters, respectively. These devices use

"non-blinding lasers" to produce "reversible optical effects,"[61] in compliance with international prohibitions on devices that cause permanent blindness.[62] Both devices have safety features that disable the laser when an object interrupts the beam within a certain distance.

Likewise, the prototype Personal Halting and Stimulation Response Rifle (PHASR) has a safety feature to prevent permanent eye damage.[63] The Air Force Research Laboratory (AFRL) developed the PHASR for use in "protecting troops and controlling hostile crowds."[64] As with any weapon—non-lethal or lethal—an enemy can develop countermeasures. For example, the effect of dazzlers may be mitigated or defeated through use of light-filtering eye protection, though the PHASR seeks to counter this by using two lasers at different wavelengths.[65] While the PHASR is an interesting, rifle-sized device, this stand-alone non-lethal dazzler weapon appears less advantageous compared to the aforementioned devices that mount onto conventional military weapons and thereby provide more than one capability. If and when a *lethal* laser weapon is developed, such "rifles" may support a hybrid mix of laser, non-lethal and/or conventional munition capabilities.

Another directed energy application does not use lasers to disorient an enemy's vision; instead, it targets the enemy's skin. AFRL developed the Active Denial System (ADS), a truck-mounted, electromagnetic radiation (microwave) device, to induce the sensation of burning skin to force an enemy to move away.[66] In 2010, ADS was deployed to Afghanistan. Unconfirmed reasons for the system's lack of use there include "ineffectiveness in bad weather; lack of penetration of thick clothing; and inability to selectively target individuals in a crowd."[67] In any event, ADS development and refinement continues, specifically with respect to making the system smaller and portable.[68]

Along with a myriad of existing and potential non-lethal weapons and devices, directed energy weapons in 2040 will provide options for CTO convoys and foot patrols in addition to conventional weapons and munitions. Options are of utmost importance when split-second, life or death decisions must be made regarding the use and escalation of force in accordance with applicable rules of engagement. While significant advances have occurred in recent years, work remains to enhance laser and microwave-based directed energy weapons to fully enable them to defeat potential countermeasures, ensure more precise target selection, and overcome environmental limitations. International and domestic concerns about usage of direct energy weapons must be assuaged as well. Still, this is a promising area for further advances in efforts to equip convoys and foot patrols with multiple ways to defend against hostile vehicles, crowds, and individuals.

Language Translation Devices

CTO personnel require real-time language translation to acquire threat information. Unarmed contract linguists provide this vital capability, at great personal risk. However, a convoy supporting numerous CTO personnel conducting various duties typically contains one or two linguists able to facilitate communication with a limited number of individuals during an engagement visit to a locality. While some CTO personnel receive "just-in-time" or even formal language training, it is usually insufficient to enable receipt of complex descriptions of threats, individuals, relationships, geography, weapons, etc. Therefore, all CTO convoy personnel need the ability to communicate effectively with the local population, which will increase the pool of individuals contacted in efforts to gain vital threat and atmospherics information.

Several technologies aim to enable real-time translation and communication between individuals speaking different languages. One recent development is the ability to connect to

language translation service providers, exemplified by the hand-held Enabling Language Service Anywhere (ELSA) device. Designed primarily for use by first responders, ELSA connects via cellular signal to a company employing interpreters for over 180 languages.[69] ELSA provides a possible model for military emulation where a pool of linguists is available on-call for use in a tactical environment. Unfortunately, this model still depends on scarce linguist resources, as well as effective communications links, and does not offer as much potential as other technologies that seek to eliminate the need for a linguist altogether. Toward this end, the US Department of Defense and commercial technology firms seek to perfect speech-to-speech translation, which provides the ability "to speak and have one's words translated automatically into the other person's language"[70] on the spot.

The Spoken Language Communication and Translation System for Tactical Use (TRANSTAC) program is a Defense Advanced Research Projects Agency effort to develop "a portable two-way speech translation system that enables an average soldier to communicate with a person who cannot speak English."[71] Since 2001, TRANSTAC evolved from one-way translation using a personal digital assistant to two-way translation via a backpack-carried laptop computer with a microphone and speaker.[72] Likewise, the US Army Machine Foreign Language Translation System (MFLTS) program is developing software for use in various portable platforms to enable two-way speech-to-speech translation and eliminate the need for a linguist in various tactical settings.[73] Judging by the limited public information available on TRANSTAC and MFLTS, it appears both programs are progressing but still not quite to the point of being able to realistically replace a linguist in the field.

Information technology giants Apple, Google, and Microsoft are also competing to develop an effective speech-to-speech capability. Each company is pursuing and promoting

software or applications ("apps") that translate spoken words from one language to another. Third-party apps for Apple devices, Google Translate, and Microsoft Bing Translator are each vying to provide the equivalent of the *Star Trek* "universal translator."[74] App-based solutions are appealing due to the ability to constantly refine translation capabilities, but this is only half the solution since a platform is still required to run the app in a field environment.

In 2040, CTO personnel will use language translation devices to more effectively communicate with local individuals. Significant gains in the field of speech-to-speech translation are currently taking place and bode well for future situations where an entire CTO team can engage, and be engaged by, individuals as necessary during outside-the-wire missions in order to more quickly gain potential threat information to prevent attacks on a deployed base.

Potential limiting factors for speech-to-speech translation devices include excessive background noise and multiple conversations in close proximity to the actual conversation requiring translation.[75] These issues will prompt constant technological refinement but will likely not pose insurmountable barriers to effective translation device usage. Additionally, translation devices will only translate language, not the non-verbal cultural cues that can be equally, if not more, important to effective tactical communication. For this reason, linguists/cultural advisors will remain an important member of the future CTO team not only to provide the most effective means to accurately translate between languages and cultures, but to also resolve discrepancies between language translation device outputs and non-verbal cues observed by the device user.

Recommendations for ESO Procurements

The USAF must pursue specific base security and CTO capabilities to counter and defeat future threats to deployed bases. To do so, the USAF must identify technological trends, harness

progress, and exploit opportunities in order to enable specific capabilities. Regardless of executive agency authority or designation as lead on a specific program, the USAF must ensure visibility on, and input into, the development of technologies and capabilities that impact ESO. Specifically, procurement decisions and planning must be geared toward acquiring technologies that enhance ESO over the next thirty years.

The USAF must continually refine anticipated capabilities requirements for future ESO to appropriately fund development and acquisition of enabling technologies. For base security, advances in counter-IDF, UGV and robotic sentry technologies reflect a general trend toward "far greater use of autonomous systems in essentially all aspects of Air Force operations."[76] Laser-based counter-IDF systems will autonomously defeat precision IDF projectiles with increased accuracy and range, while minimizing collateral damage risks. A variety of autonomous and remotely-operated UGVs carrying sensors and weaponry will enhance inside-the-wire protection and response capabilities. Posted at specific locations, non-lethal robotic sentries equipped with sensors and weaponry will autonomously detect and defeat violent insider threats. Overall, the USAF must pursue counter-IDF systems, UGVs, and robotic sentries that add base security capabilities in 2040, while reducing manpower requirements, minimizing costs, and, most importantly, mitigating risk to deployed personnel and assets.

UGV, directed energy, and speech-to-speech translation technology trends must be fully exploited to enhance and protect CTO in 2040. UGVs of sufficient survivability and load capacity will augment manned convoys and thereby enhance outside-the-wire travel and sustainment by carrying sensors and weaponry necessary for convoy security. Like base security, UGV use for CTO convoys provides more capabilities with less risk to Airmen. Directed energy weapons will improve vehicle convoy and foot patrol protection by adding

effective use of force options. Whether based on laser, microwave, or future directed energy technology, these weapons must defeat countermeasures, offer precision targeting, and overcome environmental limitations. Speech-to-speech language translation devices will enable *more* communications by CTO personnel with *more* local individuals to swiftly obtain perishable, vital threat information.

Conclusion

This research paper analyzed state-of-the-art ESO technologies and advocated for leveraging improvements in these areas to meet specific ESO capabilities requirements anticipated in 2040. This is an important area of research for future USAF expeditionary capabilities; it should prompt questions and debate, and spur further research. USAF leaders must think holistically about ESO. Although individual capabilities and technologies may seem relatively insignificant standing alone, the ability to secure personnel, aircraft, and equipment is all-important to USAF force projection in the future.

The employment of USAF airpower is critical to achieving American military objectives in support of national security strategy. Continually protecting deployed USAF resources—man and machine—is a fundamental prerequisite to successful airpower employment. Interestingly, as has been the case in recent decades, technological advances will likely continue to reduce risk to deployed personnel and equipment, which will have the ironic effect of encouraging politicians to put personnel in harm's way with more frequency in pursuit of national interests.[77] The USAF must be prepared to defend its people, aircraft, and other resources *on the ground* for future expeditionary operations deemed appropriate by civilian leadership.

---

[1] Brig Gen Robert H. Holmes et al., "The Air Force's New Ground War: Ensuring Projection of Aerospace Power through Expeditionary Security Operations," *Air & Space Power Journal* 20, no. 3 (Fall 2006): 41. "Expeditionary Security Operations" is purposely borrowed from this

influential article in order to highlight the combined proactive efforts of security forces, intelligence, and special investigations personnel to defend and secure a deployed base, whereas "Integrated Defense" is a broader term for the security forces-led sub-mission of force protection at all USAF installations. See Air Force Doctrine Document (AFDD) 3-10, *Force Protection*, 28 July 2011, 31.

[2] Due to the multitude of areas and issues that could be explored within ESO, it is important initially to acknowledge key assumptions inherent in this particular research effort in order to focus the scope and intent of this paper as it is presented: The USAF will deploy forces in the future to conduct operations in an expeditionary environment requiring basing. The USAF will not be able to solely project airpower through manned or unmanned global stand-off weapons platforms; locally-based air platforms will still be required to conduct various missions. Anti-access/area denial capabilities will not prevent the USAF from forward basing in all potential "hot spots" around the world. The USAF will deploy forces to bases of varying sizes—from large hub bases to smaller FOBs—in permissive, uncertain or hostile environments in varied climates and terrains with a range of indigenous infrastructure and security capabilities. USAF Security Forces will be responsible for security at expeditionary bases, despite shifts in responsibility at different points in time between USAF Security Forces and US Army units. The Air Force Office of Special Investigations (AFOSI) will be responsible for counter-threat operations at USAF expeditionary bases. In uncertain or hostile environments, AFOSI will conduct "outside-the-wire" operations using overt tactical vehicles for convoys to and from mission locations in the vicinity of the base.

[3] Air Force Doctrine Document (AFDD) 3-10, *Force Protection*, 28 July 2011, 1.

[4] Ibid., 31.

[5] Ibid., 29.

[6] Explanation is in order as to use of the term "expeditionary security operations." Integrated defense and FPI are excellent starting points as doctrinal terms, but they do not specifically convey the proactive, operational nature of combined Security Forces, AFOSI, and intelligence efforts to defend and secure a deployed base. For the remainder of this paper, base security and CTO will be used to differentiate between the distinct, but mutually supporting, Security Forces and AFOSI roles in ESO, in order to discuss capabilities and technologies to support both roles in the future.

[7] Air Force Instruction 31-101, *Integrated Defense*, 8 October 2009, 10.

[8] Ibid., 10-11.

[9] Air Force Doctrine Document (AFDD) 3-10, *Force Protection*, 28 July 2011, 30; Air Force Tactics, Techniques, and Procedures 3-10.3, *Integrated Defense Counterthreat Operations*, 22 December 2008, 2.

[10] Air Force Doctrine Document (AFDD) 3-10, *Force Protection*, 28 July 2011, 30.

[11] Air Force Tactics, Techniques, and Procedures 3-10.2, *Integrated Base Defense Command and Control*, 1 March 2008, 3. Brig Gen Robert H. Holmes et al., "The Air Force's New Ground War: Ensuring Projection of Aerospace Power through Expeditionary Security Operations," *Air and Space Power Journal* 20, no. 3 (Fall 2006): 43.

[12] Col Shannon W. Caudill and Maj Benjamin R. Jacobson, "Nowhere to Hide: The Growing Threat to Air Bases," *Air & Space Power Journal* 27, no. 3 (May-June 2013): 31, 33-34; Gen Norton A. Schwartz, "Airpower in Counterinsurgency and Stability Operations," *NDU Prism* 2, no. 2 (March 2011): 133.

[13] Caudill and Jacobson, "Nowhere to Hide," 34; Lt Col Thomas G. Miner, Jr., "Addressing A Gap: Shaping United States Expeditionary Air Base Defense Efforts In Support Of A Rebalance To The Pacific" (master's thesis, U.S. Air Force Air War College, 13 February 2014), 11.
[14] Ibid., 31, 37-38.
[15] I selected specific CTO capabilities and noted the threats these capabilities intend to address based on my experiences supporting and leading CTO missions in Iraq and Afghanistan in 2010 and 2012-13, respectively, and conversations with other agents with whom I had the honor to serve outside-the-wire.
[16] Any number of capabilities related to base security and CTO could be selected for future projections. Though certainly valuable for further research, many potential capabilities will not be addressed here, including those related to ballistic missile defense, defense against land attack missiles, defense against conventional enemy air assets, individual protective equipment, gear, and weapons necessary for self-defense, access controls and screening, cyberspace defense and information technology protection, etc.
[17] Office of the US Air Force Chief Scientist, *Technology Horizons: A Vision for Air Force Science and Technology 2010-2030*, (Maxwell AFB, AL: Air University Press, September 2011), xx.
[18] *Defense Industry Daily*, "A Laser Phalanx?" 23 April 2009, http://www.defenseindustrydaily.com/a-laser-phalanx-03783/ (accessed 15 February 2014).
[19] P.W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York, NY: Penguin Group, 2009), 38.
[20] Caudill and Jacobson, "Nowhere to Hide," 33-34; Schwartz, "Airpower in Counterinsurgency and Stability Operations," 133.
[21] Caudill and Jacobson, "Nowhere to Hide," 34.
[22] Rheinmetall Defence, "Oerlikon Skyshield MOOTW/C-RAM System," 21 September 2010, http://www.rheinmetall-defence.de/en/rheinmetall_defence/public_relations/news/detail_1602.php (accessed 16 February 2014); Christopher F. Foss, "Skyshield can fire far AHEAD," International Defence Exhibition & Conference 2013, 20 February 2013, http://www.ihs.com/events/exhibitions/idex-2013/news/feb-20/Skyshield-can-fire-far-AHEAD.aspx (accessed 16 February 2014).
[23] Rheinmetall Defence, "Oerlikon Skyshield MOOTW/C-RAM System."
[24] Rafael Advanced Defense Systems Ltd., "Iron Dome," http://www.rafael.co.il/marketing/SIP_STORAGE/FILES/0/1190.pdf (accessed 15 February 2014); In addition to its C-RAM capability, the Iron Dome also defends against manned and unmanned aircraft threats. The latter poses a more recent threat likely to grow in sophistication in coming years, offering another interesting avenue for additional research. See Caudill and Jacobson, "Nowhere to Hide," 34-35.
[25] Ernesto Londono, "For Israel, Iron Dome Missile Defense System Represents Breakthrough," *Washington Post*, 2 December 2012, http://www.washingtonpost.com/world/national-security/for-israel-iron-dome-missile-defense-system-represents-breakthrough/2012/12/01/24c3dc26-3b32-11e2-8a97-363b0f9a0ab3_story_1.html (accessed 15 February 2014); Jennifer Rizzo, "U.S. Continues Support for Israel's Iron Dome," Cable News Network, 17 May 2012, http://www.cnn.com/2012/05/17/us/israel-missile-system/index.html?_s=PM:US (accessed 15 February 2014).
[26] *Defense Industry Daily*, "A Laser Phalanx?"; Singer, *Wired for War*, 85.

[27] *Defense Industry Daily*, "A Laser Phalanx?"
[28] William J. Broad, "U.S. and Israel Shelved Laser as a Defense," *New York Times*, 30 July 2006, http://www.nytimes.com/2006/07/30/world/middleeast/30laser.html?_r=2& (accessed 15 February 2014).
[29] *The Week*, "The Army's eight-wheeled laser truck that zaps enemy missiles," 8 October 2012, http://theweek.com/article/index/234467/the-armys-eight-wheeled-laser-truck-that-zaps-enemy-missiles (accessed 16 February 2014); US Army Space and Missile Defense Command/Army Forces Strategic Command, "HEL TD: High Energy Laser Technology Demonstrator," http://www.smdc.army.mil/FactSheets/HEL-TD.pdf (accessed 16 February 2014).
[30] US Air Force Chief Scientist, *Technology Horizons*, 92.
[31] Prior to the conflicts in Afghanistan and Iraq, the US Congress recognized the untapped potential of UGVs, mandating that one third of ground combat vehicles be unmanned no later than 2015. See *National Defense Authorization Act for Fiscal Year 2001*, Public Law 106-398, Section 220, *U.S. Statutes at Large 114* (2001).
[32] Maj Gregory J. Nardi, "Autonomy, Unmanned Ground Vehicles, and the U.S. Army: Preparing for the Future By Examining the Past" (master's monograph, U.S. Army School of Advanced Military Studies, 21 May 2009), 41; See also US Navy Space and Naval Warfare Systems Center, "Mobile Detection Assessment and Response System (MDARS)," http://www.public.navy.mil/spawar/Pacific/Robotics/Pages/MDARS.aspx (accessed 10 February 2014).
[33] General Dynamics Robotic Systems, "Mobile Detection Assessment and Response System (MDARS)," http://www.gdrs.com/programs/program.asp?UniqueID=27 (accessed 9 February 2014).
[34] Ibid.
[35] Lt Col Brian Shoop et al., "Mobile Detection Assessment and Response Systems (MDARS) A Force Protection, Physical Security Operational Success" (US Navy Space and Naval Warfare Systems Center, 2006), 7, 9.
[36] US Navy Space and Naval Warfare Systems Center, "Mobile Detection Assessment and Response System (MDARS) II," http://www.public.navy.mil/spawar/Pacific/Robotics/Pages/MDARS2.aspx (accessed 9 February 2014).
[37] Ibid.
[38] Israel Defense Forces, "Always Watching: The IDF Unmanned Ground Vehicle," 6 December 2012, http://www.idfblog.com/2012/12/06/the-idf-unmanned-ground-vehicle/ (accessed 10 February 2014).
[39] Army Recognition, "Guardium-LS UGV G-NIUS Autonomous unmanned ground systems," http://www.armyrecognition.com/israel_israeli_wheeled_armoured_and_vehicle_uk/guardium-ls_multi_purpose_autonomous_unmanned_ground_vehicle_g-nius_ugv_israeli_army_israel_pictures.html (accessed 10 February 2014).
[40] Israel Defense Forces, "Always Watching: The IDF Unmanned Ground Vehicle."
[41] Caudill and Jacobson, "Nowhere to Hide," 40.
[42] Singer, *Wired for War*, 39.
[43] Ibid., 39.

[44] Robotics Zeitgeist, Artificial Intelligence and Robotics Blog, "Samsung Techwin's SGR-A1 robot sentry video," 14 November 2006, http://robotzeitgeist.com/2006/11/samsung-techwins-sgr-a1-robot-sentry.html (accessed 11 February 2014).
[45] Lewis Page, "South Korea to field gun-cam robots on DMZ," *The Register*, 14 March 2007, http://www.theregister.co.uk/2007/03/14/south_korean_gun_bots/ (accessed 11 February 2014).
[46] Page, "South Korea to field gun-cam robots on DMZ"; Robotics Zeitgeist, "Samsung Techwin's SGR-A1 robot sentry video."
[47] Tara Cleary, "South Korean 'super gun' packs hi-tech killing power," *Reuters*, 14 February 2011, http://www.reuters.com/video/2011/02/14/south-korean-super-gun-packs-hi-tech-kil?videoId=187406842&videoChannel=2602 (accessed 11 February 2014).
[48] Cleary, "South Korean 'super gun' packs hi-tech killing power"; Loz Blain, "South Korea's autonomous robot gun turrets: deadly from kilometers away," *gizmag*, 7 December 2010, http://www.gizmag.com/korea-dodamm-super-aegis-autonomos-robot-gun-turret/17198/ (accessed 11 February 2014).
[49] Noah Shachtman, "Israeli "Auto Kill Zone" Towers Locked and Loaded," *Wired*, 5 December 2008, http://www.wired.com/dangerroom/2008/12/israeli-auto-ki/ (accessed 11 February 2014).
[50] Ibid.
[51] Caudill and Jacobson, "Nowhere to Hide," 38.
[52] Army Recognition, "Guardium-LS UGV G-NIUS Autonomous unmanned ground systems."
[53] G-NIUS Unmanned Ground Systems, "Guardium UGV: Driven By Innovation," http://g-nius.co.il/pdf/brochures/GuardiumUGV.pdf (accessed 16 February 2014).
[54] Israel Defense Forces, "Always Watching: The IDF Unmanned Ground Vehicle."
[55] G-NIUS Unmanned Ground Systems, "Guardium UGV: Driven By Innovation."
[56] National Robotics Engineering Center, Carnegie Mellon University, "Crusher: Unmanned Ground Combat Vehicle," http://www.rec.ri.cmu.edu/projects/flyer/crusher.pdf (accessed 17 February 2014); Carnegie Mellon University Media Relations, "Carnegie Mellon's National Robotics Engineering Center Unveils Futuristic Unmanned Ground Combat Vehicles," 28 April 2006, http://www.rec.ri.cmu.edu/projects/crusher/Crusher_Press_Release.pdf (accessed 17 February 2014); Defense Advanced Research Projects Agency, "Crusher Unmanned Ground Combat Vehicle Unveiled," 28 April 2006, http://www.rec.ri.cmu.edu/projects/crusher/Crusher_Press_Release_DARPA.pdf (accessed 17 February 2014); Singer, *Wired for War*, 68. The US Army and Defense Advanced Research Projects Agency (DARPA) funded the Crusher as part of the Future Combat Systems program.
[57] National Robotics Engineering Center, Carnegie Mellon University, "Crusher Application," http://www.rec.ri.cmu.edu/projects/crusher/application/ (accessed 17 February 2014).
[58] Ibid.
[59] See US Air Force Chief Scientist, *Technology Horizons*, 30, which claims "DE [directed-energy] systems will be among the key 'game changing' technology-enabled capabilities that enter service during this time frame [2010-2030]."
[60] Department of Defense, *Non-Lethal Weapons (NLW) Reference Book* (Quantico, VA: Joint Non-Lethal Weapons Directorate, 2012), 2.
[61] Ibid.
[62] Ibid., iv.
[63] Will Knight, "US military sets laser PHASRs to stun," *New Scientist*, 7 November 2005, http://www.newscientist.com/article/dn8275#.UwKPI_KYZis (accessed 19 February 2014).

[64] Eva D. Blaylock, "New Technology Dazzles Aggressors," US Air Force Research Laboratory Directed Energy Directorate Public Affairs, 2 November 2005, http://archive.is/20120721195102/http://www.af.mil/news/story.asp?storyID=123012699#selection-707.11-436.23 (accessed 19 February 2014).
[65] Knight, "US military sets laser PHASRs to stun."
[66] Doug Hornig, "The Technological Evolution of Nonlethal Weaponry," *Casey Research*, 8 August 2013, https://www.caseyresearch.com/cdd/the-technological-evolution-of-nonlethal-weaponry (accessed 19 February 2014); Singer, *Wired for War*, 84.
[67] Hornig, "The Technological Evolution of Nonlethal Weaponry."
[68] Hornig, "The Technological Evolution of Nonlethal Weaponry"; StrategyWorld.com, "Murphy's Law: Death Ray Turns Warm And Fuzzy," 3 October 2012, http://strategypage.com/htmw/htmurph/articles/20121003.aspx (accessed 19 February 2014).
[69] Conrad Wilson, "Translation, Please: Hand-Held Device Bridges Language Gap," National Public Radio (online), 26 June 2013, http://www.npr.org/blogs/alltechconsidered/2013/06/27/186525030/translation-please-hand-held-device-bridges-language-gap (accessed 20 February 2014).
[70] Karunesh Arora, Sunita Arora, and Mukund Kumar Roy, "Speech to speech translation: a communication boon," *CSI transactions on ICT* 1.3 (2013): 207.
[71] Defense Advanced Research Projects Agency, "Translation Technology: Breaking the Language Barrier," April 2008, http://www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2676 (accessed 20 February 2014), 98.
[72] Ibid., 100-101.
[73] Michael J. Beaulieu, "US Army Machine Foreign Language Translation System (MFLTS)," October 2012, http://www.mt-archive.info/AMTA-2012-Beaulieu-abs.pdf (accessed 20 February 2014), Slide 5.
[74] Microsoft Research, "How technology can bridge language gaps: Speech-to-speech translation promises to help connect our world," http://research.microsoft.com/en-us/research/stories/speech-to-speech.aspx (accessed 20 February 2014).
[75] Brian A. Weiss and Craig I. Schlenoff, "Performance Assessments of Two-Way, Free-Form, Speech-to-Speech Translation Systems for Tactical Use," *ITEA Journal* 32 (March 2011): 72.
[76] US Air Force Chief Scientist, *Technology Horizons*, xx.
[77] Singer, *Wired for War*, 315-325.

BIBLIOGRAPHY

Air Force Doctrine Document (AFDD) 3-10. *Force Protection*, 28 July 2011.

Air Force Instruction 31-101. *Integrated Defense*, 8 October 2009.

Air Force Tactics, Techniques, and Procedures 3-10.2. *Integrated Base Defense Command and Control*, 1 March 2008.

Air Force Tactics, Techniques, and Procedures 3-10.3. *Integrated Defense Counterthreat Operations*, 22 December 2008.

Army Recognition. "Guardium-LS UGV G-NIUS Autonomous unmanned ground systems." http://www.armyrecognition.com/israel_israeli_wheeled_armoured_and_vehicle_uk/guardium-ls_multi_purpose_autonomous_unmanned_ground_vehicle_g-nius_ugv_israeli_army_israel_pictures.html (accessed 10 February 2014).

Arora, Karunesh, Sunita Arora, and Mukund Kumar Roy. "Speech to speech translation: a communication boon." *CSI transactions on ICT* 1.3 (2013): 207-213.

Beaulieu, Michael J. "US Army Machine Foreign Language Translation System (MFLTS)." Slideshow, October 2012, http://www.mt-archive.info/AMTA-2012-Beaulieu-abs.pdf (accessed 20 February 2014).

Blain, Loz. "South Korea's autonomous robot gun turrets: deadly from kilometers away." *gizmag*, 7 December 2010. http://www.gizmag.com/korea-dodamm-super-aegis-autonomos-robot-gun-turret/17198/ (accessed 11 February 2014).

Blaylock, Eva D. "New Technology Dazzles Aggressors." US Air Force Research Laboratory Directed Energy Directorate Public Affairs, 2 November 2005. http://archive.is/20120721195102/http://www.af.mil/news/story.asp?storyID=123012699#selection-707.11-436.23 (accessed 19 February 2014).

Broad, William J. "U.S. and Israel Shelved Laser as a Defense." *New York Times*, 30 July 2006. http://www.nytimes.com/2006/07/30/world/middleeast/30laser.html?_r=2& (accessed 15 February 2014).

Carnegie Mellon University Media Relations. “Carnegie Mellon’s National Robotics Engineering Center Unveils Futuristic Unmanned Ground Combat Vehicles.” 28 April 2006. http://www.rec.ri.cmu.edu/projects/crusher/Crusher_Press_Release.pdf (accessed 17 February 2014).

Caudill, Col Shannon W. and Maj Benjamin R. Jacobson, “Nowhere to Hide: The Growing Threat to Air Bases,” *Air & Space Power Journal* 27, no. 3 (May-June 2013): 30-47.

Cleary, Tara. “South Korean ‘super gun’ packs hi-tech killing power.” *Reuters*, 14 February 2011. http://www.reuters.com/video/2011/02/14/south-korean-super-gun-packs-hi-tech-kil?videoId=187406842&videoChannel=2602 (accessed 11 February 2014).

Defense Industry Daily. “A Laser Phalanx?” 23 April 2009. http://www.defenseindustrydaily.com/a-laser-phalanx-03783/ (accessed 15 February 2014).

Foss, Christopher F. “Skyshield can fire far AHEAD.” International Defence Exhibition & Conference 2013, 20 February 2013. http://www.ihs.com/events/exhibitions/idex-2013/news/feb-20/Skyshield-can-fire-far-AHEAD.aspx (accessed 16 February 2014).

General Dynamics Robotic Systems. "Mobile Detection Assessment and Response System (MDARS)." http://www.gdrs.com/programs/program.asp?UniqueID=27 (accessed 9 February 2014).

G-NIUS Unmanned Ground Systems. “Guardium UGV: Driven By Innovation.” http://g-nius.co.il/pdf/brochures/GuardiumUGV.pdf (accessed 16 February 2014).

Holmes, Brig Gen Robert H., Col Bradley D. Spacy, Lt Col John M. Busch, and Lt Col Gregory J. Reese. “The Air Force’s New Ground War: Ensuring Projection of Aerospace Power through Expeditionary Security Operations.” *Air & Space Power Journal* 20, no. 3 (Fall 2006): 41-52.

Hornig, Doug. “The Technological Evolution of Nonlethal Weaponry.” *Casey Research*, 8 August 2013. https://www.caseyresearch.com/cdd/the-technological-evolution-of-nonlethal-weaponry (accessed 19 February 2014).

Israel Defense Forces. “Always Watching: The IDF Unmanned Ground Vehicle.” 6 December 2012. http://www.idfblog.com/2012/12/06/the-idf-unmanned-ground-vehicle/ (accessed 10 February 2014).

Knight, Will. “US military sets laser PHASRs to stun.” *New Scientist*, 7 November 2005. http://www.newscientist.com/article/dn8275#.UwKPI_KYZis (accessed 19 February 2014).

Londono, Ernesto. “For Israel, Iron Dome Missile Defense System Represents Breakthrough.” *Washington Post,* 2 December 2012. http://www.washingtonpost.com/world/national-security/for-israel-iron-dome-missile-defense-system-represents-

breakthrough/2012/12/01/24c3dc26-3b32-11e2-8a97-363b0f9a0ab3_story_1.html (accessed 15 February 2014).

Microsoft Research. "How technology can bridge language gaps: Speech-to-speech translation promises to help connect our world." http://research.microsoft.com/en-us/research/stories/speech-to-speech.aspx (accessed 20 February 2014).

Miner, Lt Col Thomas G., Jr. "Addressing A Gap: Shaping United States Expeditionary Air Base Defense Efforts In Support Of A Rebalance To The Pacific." Master's thesis, U.S. Air Force Air War College, 13 February 2014.

Nardi, Maj Gregory J. "Autonomy, Unmanned Ground Vehicles, and the U.S. Army: Preparing for the Future By Examining the Past." Master's monograph, U.S. Army School of Advanced Military Studies, 21 May 2009.

National Robotics Engineering Center, Carnegie Mellon University. "Crusher: Unmanned Ground Combat Vehicle." http://www.rec.ri.cmu.edu/projects/flyer/crusher.pdf (accessed 17 February 2014)

National Robotics Engineering Center, Carnegie Mellon University. "Crusher Application." http://www.rec.ri.cmu.edu/projects/crusher/application/ (accessed 17 February 2014).

Office of the US Air Force Chief Scientist. *Technology Horizons: A Vision for Air Force Science and Technology 2010-2030*. Maxwell AFB, AL: Air University Press, September 2011.

Page, Lewis. "South Korea to field gun-cam robots on DMZ." *The Register*, 14 March 2007. http://www.theregister.co.uk/2007/03/14/south_korean_gun_bots/ (accessed 11 February 2014).

Rafael Advanced Defense Systems Ltd. "Iron Dome." http://www.rafael.co.il/marketing/SIP_STORAGE/FILES/0/1190.pdf (accessed 15 February 2014).

Rheinmetall Defence. "Oerlikon Skyshield MOOTW/C-RAM System." 21 September 2010. http://www.rheinmetall-defence.de/en/rheinmetall_defence/public_relations/news/detail_1602.php (accessed 16 February 2014).

Rizzo, Jennifer. "U.S. Continues Support for Israel's Iron Dome." Cable News Network, 17 May 2012, http://www.cnn.com/2012/05/17/us/israel-missile-system/index.html?_s=PM:US (accessed 15 February 2014).

Robotics Zeitgeist, Artificial Intelligence and Robotics Blog. “Samsung Techwin’s SGR-A1 robot sentry video.” 14 November 2006. http://robotzeitgeist.com/2006/11/samsung-techwins-sgr-a1-robot-sentry.html (accessed 11 February 2014).

Schwartz, Gen Norton A. “Airpower in Counterinsurgency and Stability Operations.” *NDU Prism* 2, no. 2 (March 2011): 127-134.

Shachtman, Noah. “Israeli “Auto Kill Zone” Towers Locked and Loaded.” *Wired,* 5 December 2008. http://www.wired.com/dangerroom/2008/12/israeli-auto-ki/ (accessed 11 February 2014).

Shoop, Lt Col Brian, Michael Johnston, Richard Goehring, Jon Moneyhun, and Brian Skibba. “Mobile Detection Assessment and Response Systems (MDARS) A Force Protection, Physical Security Operational Success.” US Navy Space and Naval Warfare Systems Center, 2006.

Singer, P.W. *Wired for War: The Robotics Revolution and Conflict in the 21st Century.* New York, NY: Penguin Group, 2009.

StrategyWorld.com. “Murphy's Law: Death Ray Turns Warm And Fuzzy.” 3 October 2012. http://strategypage.com/htmw/htmurph/articles/20121003.aspx (accessed 19 February 2014).

US Army Space and Missile Defense Command/Army Forces Strategic Command. “HEL TD: High Energy Laser Technology Demonstrator.” http://www.smdc.army.mil/FactSheets/HEL-TD.pdf (accessed 16 February 2014).

US Defense Advanced Research Projects Agency. “Crusher Unmanned Ground Combat Vehicle Unveiled.” 28 April 2006. http://www.rec.ri.cmu.edu/projects/crusher/Crusher_Press_Release_DARPA.pdf (accessed 17 February 2014).

US Defense Advanced Research Projects Agency. “Translation Technology: Breaking the Language Barrier.” April 2008. http://www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2676 (accessed 20 February 2014).

US Department of Defense. *Non-Lethal Weapons (NLW) Reference Book.* Quantico, VA: Joint Non-Lethal Weapons Directorate, 2012.

US Navy Space and Naval Warfare Systems Center. “Mobile Detection Assessment and Response System (MDARS).” http://www.public.navy.mil/spawar/Pacific/Robotics/Pages/MDARS.aspx (accessed 10 February 2014).

US Navy Space and Naval Warfare Systems Center. “Mobile Detection Assessment and Response System (MDARS) II.”

http://www.public.navy.mil/spawar/Pacific/Robotics/Pages/MDARS2.aspx (accessed 9 February 2014).

The Week. “The Army's eight-wheeled laser truck that zaps enemy missiles.” 8 October 2012. http://theweek.com/article/index/234467/the-armys-eight-wheeled-laser-truck-that-zaps-enemy-missiles (accessed 16 February 2014).

Weiss, Brian A., and Craig I. Schlenoff. “Performance Assessments of Two-Way, Free-Form, Speech-to-Speech Translation Systems for Tactical Use.” *ITEA Journal* 32 (March 2011): 69-75.

Wilson, Conrad. “Translation, Please: Hand-Held Device Bridges Language Gap.” National Public Radio (online), 26 June 2013. http://www.npr.org/blogs/alltechconsidered/2013/06/27/186525030/translation-please-hand-held-device-bridges-language-gap (accessed 20 February 2014).

ACRONYMS

ADS – Active Denial System

AFOSI – Air Force Office of Special Investigations

AFRL – Air Force Research Laboratory

BB – Base Boundary

BSZ – Base Security Zone

C-RAM – Counter-Rocket, Artillery, Mortar

CTO – Counter-Threat Operations

DARPA – Defense Advanced Research Projects Agency

DMZ – Demilitarized Zone

ECP – Entry Control Point

ELSA – Enabling Language Service Anywhere

ESO – Expeditionary Security Operations

FPI – Force Protection Intelligence

HEL TD – High Energy Laser Technology Demonstrator

IDF – Indirect Fire

IED – Improvised Explosive Device

MANPADS – Man-Portable Air Defense Systems

MFLTS – Machine Foreign Language Translation System

MDARS – Mobile Detection Assessment Response System

NATO – North Atlantic Treaty Organization

NREC – National Robotics Engineering Center

PHASR – Personal Halting and Stimulation Response Rifle

RPA – Remotely Piloted Aircraft

THEL – Tactical High Energy Laser

TRANSTAC – Spoken Language Communication and Translation System for Tactical Use

TSE – Tactical Security Element

UGV – Unmanned Ground Vehicle

US – United States of America

USAF – US Air Force